UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK

STONEX GROUP INC. and STONEX FINANCIAL INC., Plaintiffs, - against - HOWARD SHIPMAN, Defendant.	Case No. ________________

PLAINTIFFS' MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR ORDER TO SHOW CAUSE FOR A TEMPORARY RESTRAINING ORDER

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

STATUTES

Plaintiffs StoneX Group, Inc. and StoneX Financial Inc., (collectively "StoneX" or the "Company") respectfully submit this memorandum of law in support of their motion for a temporary restraining order ("TRO") against Defendant Howard Shipman ("Defendant" or "Shipman").

PRELIMINARY STATEMENT

Defendant is a former Managing Director for StoneX, where he worked as Co-Head of Quantitative Strategies within StoneX Financial Inc.'s Principal Equities Group (the "Quant Group") until his termination on December 9, 2022. Defendant was a co-developer of StoneX's new National Market System ("NMS") electronic market making project ("Pascal"), which is a highly successful, and proprietary, quantitative trading program. Following the success of Pascal, in early 2022 Defendant proposed building another trading program, called "Darwin."

As best as StoneX and its third-party forensic examiner have been able to determine to date, within minutes of StoneX firing Defendant, Defendant stole portions – if not all – of Pascal and Darwin from StoneX. Defendant exploited his access to certain StoneX servers (the "Pascal Azure servers") to remain on StoneX's systems after his access was revoked. During the roughly one-hour period that he was connected to the Pascal Azure servers after being terminated, Defendant stole 87 megabytes ("MBs") of StoneX's data and then ran a series of computer commands in an attempt to delete all traces of his conduct. Further, recent forensic examinations have uncovered that Defendant utilized at least two external hard drives to steal documents from his StoneX laptop, including files called "StoneX Docs" and "Darwin," after he was terminated. In addition, after Defendant's termination, he told a former colleague to expect a "shit show" the following Monday. StoneX discovered that Defendant sought to sabotage the Pascal program so that it would not run correctly in his absence, but StoneX was able to remedy the issue before there was any impact on Pascal.

Defendant has shown himself to be a highly skilled computer coder, crafty and brazenly non-compliant with StoneX's demands to return StoneX's confidential and trade secret information, including Pascal and Darwin. Some of the exact details of his theft have been obscured by his intentional conduct (deleting records and logs), but what is known is more than sufficient to warrant the temporary restraining order that StoneX seeks here to ensure that it does not suffer any further irreparable harm, and that its trade secrets are returned, and are not disseminated, shared, or used by Defendant or anyone on his behalf.

STATEMENT OF RELEVANT FACTS

A. StoneX's Business and the Quant Group

StoneX Group Inc. is a publicly traded financial services organization, which is listed on the NASDAQ stock exchange as SNEX. (Amato Decl. ¶ 3.) StoneX Financial Inc. is StoneX Group Inc.'s broker-dealer entity, registered with the Financial Industry Regulatory Authority ("FINRA"). (Amato Decl. ¶ 4.)

StoneX's Quant Group was established in 2021, when the Company hired Defendant and two other developers. (Amato Decl. ¶ 5.) The Quant Group makes significant investments in technology, and data subscriptions, to develop new capabilities for the Company. (Amato Decl. ¶ 6.) These projects included "Pascal", an internally developed NMS electronic market-making project, designed to provide liquidity in NMS securities. (Amato Decl. ¶ 7a.) Pascal was developed during 2021 and was operational 2022. (Amato Decl. ¶ 7a.)

Project "Darwin" is a separately developed [redacted] (Amato Decl. ¶ 7b.) Darwin was proposed and approved by the Equities Division in early 2022. While

Defendant was the developer for the program, its foundational operations relied [redacted] (Amato Decl. ¶ 7b.)

B. Howard Shipman Joins StoneX

Defendant Howard Shipman joined StoneX on February 8, 2021 as a Managing Director. (Johnson Decl. ¶ 3.) He worked remotely from his home in Connecticut during the entirety of his employment, and is a registered person with FINRA. (Johnson Decl. ¶¶ 3, 4.) Defendant signed an Employment Agreement with StoneX on February 26, 2021. (Johnson Decl. ¶ 5, Exh. 1.) Defendant's Employment Agreement included the following contractual agreements/obligations:

> Employee shall at all times perform Employee's duties faithfully and diligently and in compliance with all applicable laws, regulations, Employer written policies, and manuals provided to Employee, and any direction from Employer or from Employer's governing Board. . . . Employee also shall comply with all Employer and the Company's policies respecting ethics, trading in StoneX Group Inc. stock, and all applicable rules and regulations of the Securities and Exchange Commission. Employee shall become familiar with and shall abide by the terms of Employer's Policies, Procedures, and or Compliance Manual . . . .

(Johnson Decl. Exh. 1 at ¶ 4).

> In the event Employee's employment with the Company terminates for any reason, Employee agrees to deliver immediately to the Company all copies of materials of any nature containing any Confidential Information or otherwise regarding the Company or any customer of the Company, and Employee agrees not to take with him/her any such materials or reproductions thereof.

(Johnson Decl. Exh. 1 at ¶ 7.3(ii))

> Employee acknowledges that the services to be rendered by Employee are unique and personal. Accordingly, Employee may not assign any of Employee's rights or delegate any of Employee's duties or obligations under this Agreement. The rights and obligations of Employer under this Agreement shall inure to the benefit of and shall be binding upon the successors and assigns of Employer.

(Johnson Decl. Exh. 1 at ¶ 13).

On February 8, 2021, his first day of employment with StoneX, Defendant acknowledged and agreed to comply with the StoneX U.S. Employee Handbook dated January 2020. (Johnson

Decl. ¶ 7, Exh. 2) The StoneX U.S. Employee Handbook includes a "Confidential Company Information" provision, which states:

> The Company's confidential and proprietary information is vital to its current operations and future success. Each employee should use all reasonable care to protect or otherwise prevent the unauthorized disclosure of such information.
>
> In no event should employees disclose or reveal confidential information within or outside the Company without proper authorization or purpose. Inappropriate disclosure of confidential information may result in disciplinary action up to and including termination.
>
> "Confidential Information" refers to a piece of information, or a compilation of information, in any form (on paper, in an electronic file, or otherwise), related to the Company's business that the Company has not made public or authorized to be made public, and that is not generally known to the public through proper means.
>
> By way of example, confidential or proprietary information includes, but is not limited to, nonpublic information regarding the Company's business methods and plans, databases, systems, technology, intellectual property, know-how, marketing plans, business development, products, services, research, development, inventions, financial statements, financial projections, financing methods, pricing strategies, customer sources, employee health/medical records, system designs, customer lists and methods of competing. . . .

(Johnson Decl. ¶ 8, Exh. 2 at pp. 2-3).

C. StoneX's Computer Network Architecture and Systems

To perform its work for StoneX, the Quant Group, including Defendant, utilizes a number of physical and cloud-based technology resources. Among these resources are computers, physical servers, and cloud based servers. (Amato Decl. ¶ 15.) The Company provided Defendant with a company-owned laptop to perform his work for StoneX. (Amato Decl. ¶ 16.) However, in the time since Defendant's termination, Stonex has uncovered evidence that strongly suggests that Defendant used non-StoneX owned or approved computers, servers, and personal devices, such as his personal computer, a personally licensed Linode cloud server, and other non-StoneX devices to perform his computer-code development work for StoneX. (Wareman Decl. ¶ 21.)

Defendant also used, as authorized, a Microsoft Azure cloud servers to conduct work on behalf of StoneX. A "cloud" based server, such as Azure, does not physically sit in StoneX's facilities. Rather, it is housed and maintained by a third-party provider, which, in the case of Azure, is Microsoft. Microsoft, in turn, bills StoneX for its use of the Azure cloud servers. (Kolb Decl. ¶ 3.) The Quant Group utilized certain Azure servers that were dedicated to their projects (collectively the "Pascal Azure servers"). There are various servers, one of which is named Corvo-004. (Kolb Decl. ¶ 4.) Defendant had "administrator" privileges on the Pascal Azure servers, including Corvo-004. This meant that he was the highest-ranking user of the server, and could create, delete, and change the access, controls and privileges of the server and the account.

To access the Pascal Azure servers, Defendant used the local username "pianoman." Due to his administrator level of access, he also was able to access a permissions escalated user account on the Azure Servers, named "root". Once logged in as pianoman, Defendant could switch between the two accounts (pianoman and root) at his own discretion. (Kolb Decl. ¶ 6.)

D. StoneX Data Protection and Information Security Efforts

Because of the highly confidential and valuable nature of StoneX's business information, and in accordance with the compliance obligations imposed on StoneX by financial regulators in multiple jurisdictions across the globe, the Company utilizes many different layers and forms of information security. (Wareman Decl. ¶ 3.) Upon starting any company-owned StoneX laptop, the laptop prompts the user with the following:

> *Attention – Please Read! This computer is for StoneX business use. In line with information security, policy, all system use, including e-mail, Internet, and intranet use may be monitored to guard against unauthorized or inappropriate use. Use of this system constitutes, consent to monitoring, in accordance with local laws. Unauthorized use may result in reprimand, financial penalties, and/or legal action.*

The user must then accept this statement by clicking "ok" before logging in. (Wareman Decl. ¶ 4.)

StoneX employees are required to follow StoneX's Acceptable Use Policy ("AUP") and Acceptable Use of IT Facilities Policy ("AUFP"). (Wareman Decl. ¶ 5, Exhs. 1-2). These policies are readily available to all StoneX employees on the corporate intranet. The AUP details StoneX's expectations regarding employee protection of StoneX's data, information, systems, networks and computers. The AUP includes requirements to ensure information security, such as: (a) prohibiting unauthorized access to accounts (including stealing or misusing a password), programs and/or data, (b) requiring that StoneX's proprietary information stored on electronic and computing devices whether owned or leased by StoneX, the employee or a third party, remains the sole property of StoneX, (c) requiring that data owned, processed or held by the Company, must be protected in accordance with data protection standards, and (d) disclosing that the Company may log all forms of employee IT use and communications, and that the Company reserves the right to monitor computer equipment, systems and network traffic. (Wareman Decl. ¶ 6.)

Section 1.0 of the AUP provides that computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, and FTP remain the property of StoneX. (Wareman Decl. ¶ 7.) Section 3.5 of the AUP maintains that accessing data, a server or an account for any purposes other than conducting StoneX business is prohibited. (Wareman Decl. ¶ 8.)

Section 3.8 of the AUFP provides StoneX's Exit Procedures, which states:

> Upon leaving the Company it is expected that users:
>
> - Promptly return all Company IT equipment in reasonable working condition.
> - Do not delete any data which belongs to the Company.
> - Transfer any data which may be needed by the Company to an appropriate server or colleague prior to departure.

- Ensure any of their own data that they wish to keep is removed from the Company's systems, as they will not be entitled to access this once they leave.
- Review and conform to any other procedures set out by the Company in relation to departure.

(Wareman Decl. ¶ 9.)

In addition to Company policies, StoneX Group Inc. employs approximately 80 individuals globally to ensure the Company's cyber security. These employees operate via various teams, including Identity & Access Management, Cybersecurity/Security Operations, IT Governance, Risk & Compliance, Third Party Vendor Risk and Business Resiliency. StoneX also employs a stand-alone internal audit team, which exists outside of StoneX's cyber security group and reports directly to StoneX's executive committee. Among other things, this team conducts independent audits of StoneX's cyber security systems. (Wareman Decl. ¶¶ 10-11.) Further, StoneX performs regular third-party penetration testing to ensure the security of its network. (Wareman Decl. ¶ 12.)

StoneX ensures employee desktops, laptops, mobile devices, servers, and databases are initially configured to meet the Company's cyber security requirements. (Wareman Decl. ¶ 13.) To log on to StoneX's network, employees can utilize a virtual private network ("VPN"), which is an online portal used to access StoneX's network, or connect directly from one of StoneX's physical offices using an authorized device. VPN login requires a username, password, multi-factor verification and an authorized StoneX device. Access to StoneX's network from within a StoneX office requires the use of a username, password and authorized StoneX device. (Wareman Decl. ¶ 14.)

Across its entire network, StoneX utilizes the 'least privilege' principle, which means that StoneX employees only have access to the data or information that they need to perform their job. (Wareman Decl. ¶ 16.) StoneX's confidential information is heavily guarded. In addition to all of the other security measures in place throughout StoneX's network, the Company utilizes additional monitoring, vulnerability management and remediation programs to ensure the protection of this information. (Wareman Decl. ¶ 17.)

Upon information and belief, Defendant was fully aware of StoneX's cyber security policies and procedures. (Wareman Decl. ¶ 18.) Between September 2021 and March 2022 StoneX's Cyber Security Architect Frank McGovern and Michael Glatz, Manager of Security Engineering, spent hours speaking directly with Defendant about the various rules and regulations of cyber security compliance that were applicable to him and his team, including sharing copies of policies applicable to the environment. (Wareman Decl. ¶ 19.)

E. Development and Use of Pascal

Project "Pascal" is StoneX's new NMS electronic market making project, and the computer code for Pascal is a highly valuable piece of proprietary software. [redacted] (Amato Decl. ¶ 7a.) StoneX invested millions of dollars to develop this trading system, including for equipment, staff, leased co-location spaces, lines, and market data. (Amato Decl. ¶ 7a.) Pascal became operational in 2022 and generated substantial revenue in 2022. (Amato Decl. ¶ 7a.)

The Pascal code is comprised of three main code libraries, named: "Alabama," "Texas," and "Tampa." (Pfeuffer Decl. ¶ 3.) At a high level: [redacted] These components that make up Pascal are stored in a code "repository," which is an archive of computer source code, stored on servers (cloud or physical). (Pfeuffer Decl. ¶ 5.) Defendant was the developer of Texas. (Pfeuffer Decl. ¶ 7.)

F. Development of Darwin

Following completion of the operational code for Pascal, StoneX began development of Darwin in early 2022. (Amato Decl. ¶ 8.) Darwin was designed to: [redacted] All of the computer code for Darwin was intended to be – and was in fact – developed by StoneX employees. (Pfeuffer Decl. ¶ 9.) [redacted] (Amato Decl. ¶ 10.) Darwin was to be developed (*i.e.,* the code should have been written and stored) on the StoneX Pascal Azure servers in accordance with StoneX's policies. (Amato Decl. ¶ 11.)

Throughout 2022, the development of "Darwin" had advanced significantly enough that on December 9, 2022, Defendant's termination date, he provided a virtual presentation of Darwin to the Quant Team. In that presentation, Defendant:

a) Demonstrated Darwin's operation in a test environment,

b) Presented portions of Darwin's source code,

c) Edited, compiled and re-ran portions of the source code to demonstrate its use and specific features including the design, editing and running of a new calculator, and

d) Stated that he would be sharing the source code with the rest of the team later that day or Monday, December 12th. (Pfeuffer Decl. ¶ 14.)

Indeed, although still in the development stage, StoneX has already committed several million dollars towards the necessary hardware, data centers, and information necessary for Darwin's future operation. (Amato Decl. ¶ 7b.)

Critically, in the time since Defendant's termination, and after extensive investigation and discussions with other members of the Quant Team, StoneX has been unable to locate a copy of the Darwin source code as presented on December 9th on any of StoneX's systems or repositories. (Pfeuffer Decl. ¶ 15.) Upon information and belief, Defendant did not share a copy of the Darwin source code with anyone at StoneX. (Pfeuffer Decl. ¶ 16.) He promised Pfeuffer on multiple occasions that he would share the Darwin code with Pfeuffer, but as of his termination he did not. (Pfeuffer Decl. ¶ 16.)

G. StoneX Terminated Shipman on December 9, 2022

StoneX terminated Defendant's employment on December 9, 2022. (Johnson Decl. ¶ 9.) StoneX management directed IT to begin terminating Defendant's authorized StoneX's account at approximately 3:09pm CST on December 9, 2022. (Johnson Decl. ¶ 10.) StoneX's Front Office Management Team and Anne Johnson (Global HR Business Partner) contacted Defendant twenty minutes later to advise that he was being terminated effective immediately via a telephone call at approximately 3:30pm CST on December 9, 2022. The call lasted approximately 10 minutes. (Johnson Decl. ¶ 11.)

StoneX's security team coordinated to terminate Defendant's access to its systems and network – before Defendant was notified of his termination. However, unbeknownst to StoneX, Defendant maintained and unauthorized, pre-existing connection to the Pascal Azure servers from a personal cloud server (the "Linode server") with IP address [redacted] ("Shipman's IP Address"), which allowed him to remain on the network. (Wareman Decl. ¶¶ 21-22.) Specifically, on December 9, 2022, Defendant logged into the Pascal Azure servers from the Linode server, rather than his StoneX issued laptop, at roughly 8:58am CST. He then remained logged into the Pascal Azure servers until 4:45pm CST that evening.

H. Shipman Steals StoneX Code and Tries to Cover His Tracks

After his termination, Defendant maintained his connection to StoneX's systems via his personal Lenode server for more than an hour. During this period he continued not only to access data, but he also manipulated and egressed StoneX data and information. (Wareman Decl. ¶¶ 26.) In fact, between 3:30pm and 4:45pm CST, Defendant used his access to StoneX's systems to execute an unknown number of commands, deletions, and/or other actions, culminating in his extraction of 87 megabytes ("MBs") of data from StoneX's server. 87MBs is slightly larger than the Pascal repository (roughly 70MBs) that was archived on the Pascal Azure servers at the time of the data egress. (Kolb Decl. ¶ 8.)

Also during this period, following the egress of data, at approximately 4:05pm CST, Defendant (*i.e.* pianoman) deleted his server "bash history," from November 7, 2022 onwards, from the Pascal Azure server named Corvo-004. (Wareman Decl. ¶ 27.) The "bash history" is a log of all prior coding commands utilized on a server that would reveal all of his actions. (Wareman Decl. ¶ 27.) Shortly thereafter, Defendant switched from his "pianoman" account to the "root" account. At 4:13pm CST, the administrator level "root" account, under Defendant's control, deleted the bash history associated with any actions taken by it. (CRA Decl. ¶ 31.) The StoneX security team was alerted to this activity as two security alerts were raised after Shipman's termination for history files being cleared by the account "pianoman" and "root" at 4:05pm CST and 4:13pm CST. (Wareman Decl. ¶ 32.) Without the bash histories, StoneX is unable to determine (a) exactly what was included in the 87MBs that Defendant egressed, and (b) where it was sent. However, StoneX is working with a forensics firm (Charles River Associates) to investigate this and other questions. (Wareman Decl. ¶ 34.)

Notably, in the time since Defendant's termination, StoneX was able to locate a folder in the Pascal Azure servers named "Darwin," but it was empty. (Kolb Decl. ¶ 10.) Additionally, after

Defendant's termination at 3:30pm CST and final logoff of his login from his Linode server at approximately 4:45pm CST on December 9, 2022, Defendant made additional attempts to access StoneX's network that evening and throughout the weekend. (Wareman Decl. ¶ 33.)

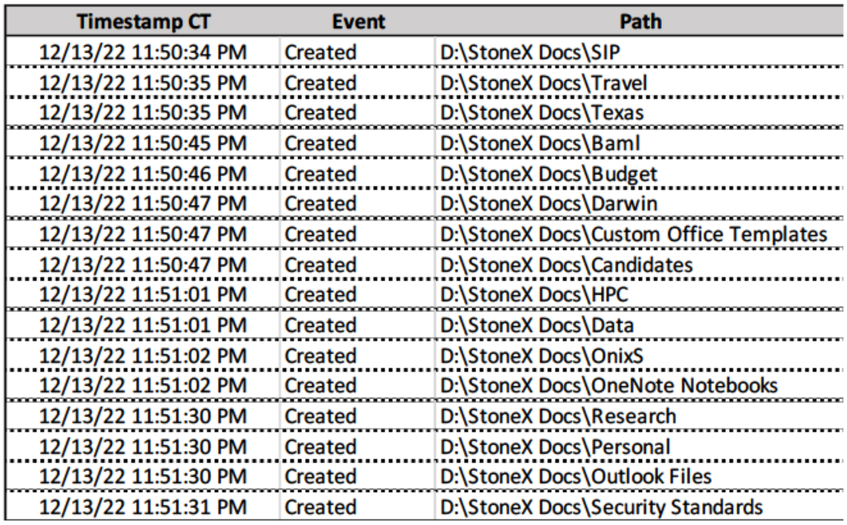
I. Forensic Work on Shipman's Laptop

StoneX's outside counsel, Proskauer Rose, hired Charles River Associates ("CRA") on behalf of StoneX to perform forensic examinations of StoneX's computer systems, and Defendant's StoneX laptop. (Wareman Decl. ¶ 34.) CRA was retained on or about December 27, 2022. Due to the delay by Defendant in returning his StoneX laptop, CRA only received the laptop during the day on January 3, 2022. (Wareman Decl. ¶ 35.) To date, StoneX has spent more than $5,000.00 in order to (a) respond to Defendant's conduct and (b) pay CRA to conduct its damage assessment of the data taken from Defendant's computer. (Wareman Decl. ¶ 36.)

To date, CRA collected from StoneX and identified/reviewed via forensic software: (a) computer system logs and records associated with Defendant; (b) Defendant's StoneX laptop, and (c) a "virtual computer" hosted within the Corvo-004 Pascal Azure server, which Defendant appears to have utilized for StoneX work. (CRA Decl. ¶¶ 10-14.)

Critically, in addition to the egress of 87 MBs of data from the Pascal Azure servers, CRA's review of Defendant's StoneX laptop also revealed that he stole further StoneX data after he was terminated. Specifically, on December 10, 2022 at 10:55:15 am CST, a SanDisk drive (an external hard drive) was connected to Defendant's StoneX laptop. Defendant's StoneX laptop assigned the SanDisk drive a device name of "SanDisk Cruzer Glide USB Device" and an internal serial number of "20042605701683737105". The storage volume on the SanDisk drive was named "UBUNTU-SERV". (CRA Decl. ¶ 21.)

On December 13, 2022 at 11:47:47pm CST, Defendant connected the SanDisk drive to his StoneX laptop. At 11:49:54pm CST, Defendant created the folder "StoneX Docs" on the SanDisk drive. (CRA Decl. ¶ 22.) From 11:50:34 pm until 11:51:31pm CST, folders with the names "StoneX Docs\Texas," "StoneX Docs\Darwin," "StoneX Docs\Research" and "StoneX Docs\Budget," among others, were copied to the SanDisk drive.



Timestamp CT	Event	Path
12/13/22 11:50:34 PM	Created	D:\StoneX Docs\SIP
12/13/22 11:50:35 PM	Created	D:\StoneX Docs\Travel
12/13/22 11:50:35 PM	Created	D:\StoneX Docs\Texas
12/13/22 11:50:45 PM	Created	D:\StoneX Docs\Baml
12/13/22 11:50:46 PM	Created	D:\StoneX Docs\Budget
12/13/22 11:50:47 PM	Created	D:\StoneX Docs\Darwin
12/13/22 11:50:47 PM	Created	D:\StoneX Docs\Custom Office Templates
12/13/22 11:50:47 PM	Created	D:\StoneX Docs\Candidates
12/13/22 11:51:01 PM	Created	D:\StoneX Docs\HPC
12/13/22 11:51:01 PM	Created	D:\StoneX Docs\Data
12/13/22 11:51:02 PM	Created	D:\StoneX Docs\OnixS
12/13/22 11:51:02 PM	Created	D:\StoneX Docs\OneNote Notebooks
12/13/22 11:51:30 PM	Created	D:\StoneX Docs\Research
12/13/22 11:51:30 PM	Created	D:\StoneX Docs\Personal
12/13/22 11:51:30 PM	Created	D:\StoneX Docs\Outlook Files
12/13/22 11:51:31 PM	Created	D:\StoneX Docs\Security Standards

CRA searched Defendant's StoneX laptop for these folders but was unable to locate or forensically recover these folders or data they may have contained. (CRA Decl. ¶ 23.)

Defendant utilized a second external hard drive to steal materials from StoneX. On December 26, 2022 at 3:45:53 pm CST, another external hard drive, made by Sony, was connected to Defendant's StoneX laptop. (CRA Decl. ¶ 29.) Defendant's laptop assigned the Sony drive a device name of "Sony Storage Media USB Device" and an internal serial number of "7&388e6bd2." (CRA Decl. ¶ 29.) Sixty-three seconds after the Sony drive was connected to Defendant's StoneX laptop, two files were accessed: "C:\Users\howard.shipman\Documents\Darwin\QuantStrat Plan 2023.docx" and "C:\Users\howard.shipman\Documents\mm_shares.xlsx". These events are consistent with the two files being copied to the Sony drive. The Sony drive was then removed from Defendant's laptop on December 26, 2022 at 4:06:15pm CST. (CRA Decl. ¶ 30.)

The "QuantStrat Plan 2023" document and "mm_shares" documents are highly sensitive and confidential to StoneX. (Amato Decl. ¶ 18-19.) The "QuantStrat Plan 2023" document is marked "Strictly Confidential and Private, Property of StoneX," and includes detailed information about StoneX's strategy, monetization strategy and market predictions, for the Quant Group. (Amato Decl. ¶ 18) The "mm_shares" document is a Microsoft Excel file that includes sensitive and confidential financial projections for StoneX's market-making activities. (Amato Decl. ¶ 19.) This information is unique to StoneX and its target goals. (Amato Decl. ¶ 19.)

In addition, on December 14, 2022 at 12:00:35am CST, a "VirtualBox" folder and any files it contained were deleted from Defendant's StoneX Laptop. (CRA Decl. ¶ 24.) VirtualBox is a software program that creates and runs virtual versions of computers on other computers. (CRA Decl. ¶ 25.) Any virtual computers and information about those virtual computers that are typically stored within the VirtualBox folder were deleted by Defendant.

CRA also discovered that on December 23, 2022 at 2:39pm CST, all Google Chrome web history was cleared from Defendant's StoneX laptop. (CRA Decl. ¶ 28.) Clearing the web history removes the history of web sites that were visited, saved passwords, and other web browser data and settings. CRA was unable to recover any Google Chrome external web browsing history data from Defendant's StoneX laptop because it was cleared. (CRA Decl. ¶ 28.) StoneX has uncovered no information, however, which indicates that Shipman has taken information relating to its customers or counterparties.

J. Further Evidence of Shipman's Malicious Intent and Deception

Following Defendant's termination, on December 10, 2022, Pfeuffer contacted Defendant to say 'goodbye'. (Pfeuffer Decl. ¶ 17.) During that phone call, Defendant stated that StoneX should expect a "shit show" on Monday morning. When Pfeuffer asked Defendant what he meant, or if Defendant would help or StoneX avoid the impending "shit show," Defendant refused to help and stated that he would do nothing to assist StoneX or Pfeuffer. (Pfeuffer Decl. ¶ 18.) Pfeuffer asked for Defendant's assistance, or even just guidance into the cause of the "shit show," but Defendant refused. (Pfeuffer Decl. ¶ 18.) StoneX shortly thereafter discovered that Shipman had sabotaged Pascal so that it would not run correctly in his absence. Fortunately, StoneX was able to resolve the issue without any disruption to the running of Pascal. (Pfeuffer Decl. ¶ 19.)

ARGUMENT

StoneX is Entitled to a Temporary Restraining Order Enjoining Defendant from Further Misappropriating Its Trade Secrets.

A temporary restraining order is appropriate where the movant shows (1) a likelihood of success on the merits or sufficiently serious questions going to the merits to make them a fair ground for litigation and a balance of hardships tipping decidedly in the plaintiff's favor; (2) a likelihood of irreparable injury in the absence of an injunction; (3) that the balance of hardships tips in the plaintiff's favor; and (4) that the public interest would not be disserved by the issuance of an injunction. *Benihana, Inc. v. Benihana of Tokyo, LLC*, 784 F.3d 887, 895 (2d Cir. 2015) (citation omitted). "[T]he standard for an entry of a temporary restraining order is the same as for a preliminary injunction." *AFA Dispensing Grp. B.V. v. Anheuser-Busch, Inc.*, 740 F. Supp. 2d 465, 471 (S.D.N.Y. 2010); *Roso-Lino Beverage Distribs., Inc. v. Coca-Cola Bottling Co.*, 749 F.2d 124, 125-26 (2d Cir. 1984). Here, the evidence is overwhelming that StoneX meets all of the elements necessary for the Court to grant a temporary restraining order.

A. StoneX Is Likely To Succeed On The Merits Of Its Claims

StoneX is likely to succeed on the merits of its claims against Defendant for (1) violation of the Defend Trade Secrets Act ("DTSA"); (2) violation of the Computer Fraud and Abuse Act ("CFAA"); (3) misappropriation of trade secrets under New York law; and (4) breach of fiduciary duty. To establish a likelihood of success on the merits, a plaintiff need only show that it is more likely than not that it will prevail on its claims. *Nat'l Elevator Cab & Door Corp. v. H&B, Inc.*, 282 F. App'x 885, 888 (2d Cir. 2008). An applicant for injunctive relief "need only make a showing that the probability of his prevailing is better than fifty percent." *Broker Genius, Inc. v. Zalta*, 280 F. Supp. 3d 495, 510 (S.D.N.Y. 2017) (quoting *Eng v. Smith*, 849 F.2d 80, 82 (2d Cir. 1988)). Given Defendant exploited, accessed, manipulated, and extracted StoneX's intellectual property and trade secrets after his termination, StoneX will likely succeed on the merits for its claims against Defendant.

Count I: Violation of the DTSA.

StoneX is likely to prevail on the merits of its DTSA claim because the information extracted from StoneX's systems, the Pascal Azure servers and Defendant's StoneX Laptop (1) is classified as a trade secret and (2) was acquired by Defendant through improper means. The DTSA creates a private cause of action in favor of the owner of a trade secret that is misappropriated "if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C. § 1836(b)(1). Under the DTSA, a trade secret includes:

> all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if –
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information[.]

18 U.S.C. § 1839(3).

"Misappropriation" under the DTSA includes "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means" or "disclosure or use of a trade secret of another without express or implied consent" in specified circumstances. 18 U.S.C. § 1839(5)(A)–(B). The phrase "improper means" includes "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means[.]" 18 U.S.C. § 1839(6)(A); *Intertek Testing Servs., N.A. v. Pennisi*, 443 F. Supp. 3d 303, 340 (E.D.N.Y. 2020). Here, StoneX meets both elements to prove a claim under the DTSA.

First, Defendant extracted and took highly confidential and trade secret information from StoneX. Immediately after StoneX terminated his employment, effective immediately, Defendant extracted of 87 MBs of data from StoneX's server. This is the same server that held the Pascal repository, and is slightly larger in size than the Pascal repository. Defendant then did everything in his power to cover his tracks, by deleting his "bash history."

Next, one day after Defendant's termination, Defendant connected the SanDisk drive to his StoneX-issued laptop and subsequently copied folders, including those titled "StoneXDocs\Budget", "StoneXDocs\Custom Office Templates", "StoneXDocs\Darwin", "StoneXDocs\Data", "StoneXDocs\Research" and "StoneXDocs\Texas". (CRA Decl. ¶ 22.) Defendant also connected a Sony drive to his laptop on December 26, 2022 and accessed the files "QuantStrat Plan 2023" and "mm_shares" – comprising StoneX's quantitative strategy plan for 2023, and key metrics and market revenue targets. (CRA Decl. ¶ 29-30.)

The 87 MBs that were egressed from Corvo-004, and the folders and files that Defendant took from his StoneX laptop and placed on the SanDisk drive and the Sony drive, constitute StoneX's financial, business, and technical information. They contained (1) StoneX's Pascal trading program (including the code for "Texas", which includes the [redacted] for

Pascal); (2) StoneX's future trading program "Darwin"; and (3) proprietary financial information for StoneX's business. (CRA Decl. ¶ 22.)

Further, following Defendant's termination and after investigation, StoneX has been unable to locate a copy of the Darwin source code as presented on the December 9th on any of the Pascal Azure servers or any of StoneX's systems or repositories. (Pfeuffer Decl. ¶ 15.) Therefore, under the DTSA, the information egressed from Defendant's StoneX computers to the SanDisk and Sony drive are classified as trade secrets.

Courts have previously held that predictive algorithms (such as Pascal and Darwin) are trade secrets under both the DTSA and CFAA. *LivePerson, Inc. v. 24/7 Customer, Inc.*, 83 F. Supp. 3d 501, 515 (S.D.N.Y. 2015) (finding the plaintiff's predictive algorithms and proprietary behavior analysis methods that were based on extensive research and undertaken with great expense to constitute trade secrets); *Secured Worldwide LLC v. Kinney*, No. 15 Civ. 1761(CM), 2015 WL 1514738, at *15 (S.D.N.Y. Apr. 1, 2015) ("[the plaintiff's] business model would not be able to operate without the algorithm" and therefore the algorithm constituted a trade secret.) In *United States v. Aleynikov*, the court found the court found a high-frequency trading system, which utilized an algorithm to perform analyses of past trades, to be a "product" within the meaning of the CFAA, and that the trade secret at issue was the trading system's source code. 737 F. Supp. 2d 173, 177-78 (S.D.N.Y. 2010). Similar to the facts here, the defendant in *Aleynikov* on his last day of employment, copied, compressed, encrypted, and transferred to an outside server thousands of source code and deleted his "bash history" from his server. *Id.* at 175. The court concluded the defendant overwhelmingly accessed his former employer's trading systems that were classified as trade secrets. *Id.* at 177-78.

Further, StoneX invested in equipment, staff, leased co-location spaces, lines, and market space to support the development of Pascal, including the investment of millions of dollars to develop. (Amato Decl. ¶ 7a.) Pascal code was written on StoneX's Pascal Azure server, and the compiled, executable version operates from StoneX's physical servers. (Pfeuffer Decl. ¶ 8.) Moreover, the computer code for Darwin was developed by StoneX employees, and initially relied [redacted]. (Pfeuffer Decl. ¶ 12.) While still in development, StoneX has already committed several million dollars to the necessary hardware, data centers, and information necessary for Darwin's operation. (Amato Decl. ¶ 7b.)

StoneX also took reasonable measures to protect its valuable trade secrets. Among the many security measures in place, Stone X employs approximately 80 individuals globally to ensure StoneX's cybersecurity; requires a virtual private network with a username, password and multi-step verification to log on to StoneX's network; employs the "least privilege principle" to ensure StoneX employees may only access data or information they need to perform their job; uses the best-in-class EDR tools to detect and investigate threats to its network; and ensures constant monitoring, vulnerability management, and remediation programs to ensure the protection of StoneX's information. (Wareman Decl. ¶¶ 10, 15-17.) Simply put, the code for Pascal and Darwin plus StoneX's financial information were heavily safeguarded.

Second, Defendant misappropriated StoneX's trade secrets by "improper means" as defined by the DTSA. 18 U.S.C. § 1839(5)(a). The term "improper means" includes not only "theft" and "misrepresentation," which would apply here, but also "breach or inducement of a breach or duty to maintain secrecy." *Id.* By duplicitously removing files for his personal use, Defendant "breach[ed] . . . a duty to maintain secrecy[.]" 18 U.S.C. § 1839(6)(A); *KCG Holdings, Inc. v. Khandekar*, No. 17-CV3533(AJN), 2020 WL 1189302, at *10 (defendant used improper means to acquire and use trade secrets when, in violation of his employer policy, he copied, reviewed, and organized files into his personal directory); *AUA Priv. Equity Partners, LLC v. Soto*, No. 1:17-cv-8035-GHW, 2018 WL 1684339, at *7 (S.D.N.Y. Apr. 5, 2018) (misappropriation by acquisition plausibly alleged with claims that defendant "uploaded [plaintiff's] trade secrets from her work laptop to her personal cloud-based storage without [plaintiff's] permission and in direct violation of the confidentiality agreements that she signed"). Here, Defendant took – after he was already terminated – 87 MBs of highly sensitive information from StoneX's servers and connected two external hard drives to remove StoneX folders titled "Darwin", "Research" and "Texas," from his work laptop. (CRA Decl. ¶ 22.) Such extraction constitutes "theft" under the DTSA and was a breach of Defendant's duty to maintain secrecy.

In addition to the extracted materials, Defendant also deleted information to cover his tracks and prevent StoneX from determining where Defendant took the information. On December 9, 2022 at 4:05pm CST, one hour after Defendant's termination, the Microsoft Azure Defender security alert reported the "bash_history" for Defendat's "pianoman" account was deleted. (CRA Decl. ¶ 17.) Only a few minutes later, the Microsoft Azure Defender security alert reported the bash_history for Defendant's "root" account was deleted as well. CRA also confirmed that the bash_history for "pianoman" and "root" were cleared using the "VIM" text editor. (CRA Decl. ¶ 19.) Folders under the pianoman account, including "Desktop, Downloads, and Documents" were similarly deleted in the hour after Defendant's termination. (CRA Decl. ¶ 20.) Further, on December 14, 2022, Defendant deleted the "virtual box" folder and any files – essentially a computer within a computer where Defendant performed work for StoneX on its trading strategies – contained within from StoneX laptop. (CRA Decl. ¶ 24.)

Notably, Defendant's Employment Agreement provides that in the event of termination, Defendant should "deliver immediately to the Company all copies of materials of any nature containing any Confidential Information" and "not to take with him any such materials or reproductions therefore." (Johnson Decl. ¶ 6.) Further, StoneX's Acceptable Use Policy includes requirements to ensure information security, such as: (a) prohibiting unauthorized access to accounts (including stealing or misusing a password), programs and/or data and all forms of hacking, (b) requiring that data owned, processed or held by the Company, must be accessed, stored, processed and backed up in a manner appropriate to its security classification, (c) requiring that employees only use services provided or endorsed by the Company for conducting Company business, and (d) disclosing that the Company may log all forms of employee IT use and communications, and that he Company reserves the right to inspect any items of computer equipment connected to the StoneX network. (Wareman Decl. ¶ 6.) Defendant's extraction and deletion of his bash history clearly violates both his Employment Agreement and StoneX's Acceptable Use of IT Facilities Policy and constitutes misappropriation under the DTSA.

Thus, Defendant misappropriated StoneX's trade secrets through improper means and in violation of his duties to StoneX. Therefore, StoneX is likely to succeed on the merits of its DTSA claim.

Count II: Violation of the CFAA

StoneX is likely to succeed in proving that Defendant violated the CFAA by intentionally accessing at least one of StoneX's protected computers without authorization to such computer, causing StoneX to suffer a loss in an amount exceeding $5,000. 18 U.S.C. § 1030(a)(2)(C). Under the CFAA, a "protected computer" is defined as a computer "which is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). Damage is defined as "any impairment to the integrity or availability of data, a program, a system, or information," and loss is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage, assessment, and restoring the data to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of disruption of service." 18 U.S.C. § 1030 (e)(8), (11). Courts have recognized that the costs of investigating security breaches constitute recoverable losses, even if turns out that no actual data damage or interruption of servicer resulted from the breach. *Dreni v. PrinterOnAmerica Corp.*, 468 F. Supp. 3d 712, 735 (S.D.N.Y. 2020); *Univ. Sports. Publ'ns Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 387 (S.D.N.Y. 2010).

Here, StoneX satisfies the elements to plead a claim under the CFAA. Both the Pascal Azure server and Defendant's StoneX laptop are considered "protected" under the CFAA because they were used in or affecting interstate commerce and communication. 18 U.S.C. § 1030(e)(2)(B). Second, Defendant clearly accessed the Pascal Azure servers "without authorization" immediately after his "effective immediately" termination. StoneX's security team coordinated to terminate Defendant's access to its systems network ***before*** Defendant received notification of his termination. (Wareman Decl. ¶ 26.) In fact, StoneX management directed IT to begin termination Defendant's authorized StoneX account approximately 20 minutes before his termination. (Johnson Decl. ¶ 10.) However, Defendant was still able to maintain a connection via Shipman's IP Address and continued to access (and delete) data from StoneX's servers. (Wareman Decl. ¶ 26.) Defendant had no authorization to access the Pascal Azure server after 3:30pm SCT on December 9, 2022, yet repeatedly did so for 75 minutes following his termination. (Wareman Decl. ¶ 27.) Defendant also attempted to access StoneX's computers throughout the evening on December 9, 2022 and through the weekend, despite StoneX security revoking his access.

(Wareman Decl. ¶ 33.) Similarly, Defendant accessed his StoneX laptop "without authorization" by connecting two external hard drives to the computer after he had already been terminated, and deleting the "virtual box" on that computer. (CRA Decl. ¶¶ 22, 24, 26.) Therefore, Defendant accessed StoneX's protected computers without authorization.

Finally, Defendant caused losses to StoneX of more than $5,000. To date, StoneX has spent more than $5,000 in order to: (a) respond to Defendant's conduct and (b) pay CRA to conduct its damage assessment of the data taken from Defendant's computer. (Wareman Decl. ¶ 36.) Such retention constitutes a "loss" to StoneX under the CFAA, and StoneX has incurred more than $5,000 in fees from CRA. *See Dreni*, 478 F. Supp. 3d at 735. Because StoneX meets all of the elements necessary under the CFAA, StoneX is likely to succeed on the merits in proving its claim.

Count III: Misappropriation of Trade Secrets under New York Common Law.

StoneX's claim that Defendant misappropriated trade secrets under New York common law is also likely to prevail. Because "[t]he elements for a misappropriation claim under New York law are fundamentally the same" as a DTSA claim, "courts have found that a '[c]omplaint sufficiently plead[ing] a DTSA claim . . . also states a claim for misappropriation of trade secrets under New York law.'" *Iacovacci v. Brevet Holdings, LLC*, 437 F. Supp. 3d 367, 380 (S.D.N.Y. 2020) (quoting *ExpertConnect, L.L.C. v. Fowler*, No. 18 Civ. 4828(LGS), 2019 WL 3004161, at *7 (S.D.N.Y. July 10, 2019)). To succeed on a claim for the misappropriation of trade secrets under New York law, a party must demonstrate that: (1) it possessed a trade secret, and (2) the defendant used that trade secret in breach of an agreement, confidential relationship or duty, or as a result of discovery by improper means. *Faiveley Transp. Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 117 (2d Cir. 2009) (applying New York law).

Here, Defendant possessed and continues to possess StoneX's confidential and trade secret information, including – it strongly appears – the computer code for Pascal and Darwin and the "QuantStrat Plan 2023" and "mm_shares" documents. In addition to the 87 MBs that Defendant extracted, Defendant also currently possess at least two external hard drives with StoneX's information that Defendant extracted from his StoneX laptop. (CRA Decl. ¶ 22, 29.)

Defendant misappropriated StoneX's trade secrets and confidential business information through improper means in breach of his fiduciary duty to the Company (*see* Count IV below) as a managing director. Defendant's extraction of StoneX's information is in violation of his Employment Agreement signed at the beginning of his employment with StoneX and StoneX's Acceptable Use of IT Facilities Policy. (Johnson Decl. ¶ 6, Wareman Decl. ¶¶ 6-9.) Thus, for the same reasons as the DTSA claim, StoneX is likely to prevail on its claim that Defendant misappropriated StoneX's trade secrets in violation of New York common law.

Count IV: Breach of Fiduciary Duty.

StoneX is also likely to succeed in establishing that Defendant breached his fiduciary duty. To establish a claim for breach of fiduciary duty, a plaintiff must show (1) the existence of a fiduciary relationship, (2) misconduct by the other party, and (3) damages directly caused by that party's misconduct. *Informa Bus. Intelligence, Inc. v. Reich*, No. 657534/2019, 2022 WL 4080615, at *3 (Sup. Ct. N.Y. Cty. Sept. 6, 2022). Under New York law, "the employer-employee relationship is fiduciary." *UAB, Inc. v. Ethos Auto Body, LLC*, No. 70850/2018, 2021 WL 4430646, at *10 (Sup. Ct. Westchester Cty. Mar. 9, 2021); *Zurich Am. Life Ins. Co. v. Nagel*, 538 F. Supp. 3d 396, 403 (S.D.N.Y. 2021) ("Under New York law, employees owe fiduciary duties to their employers, independent of any contractual duties, and some such duties survive termination."). Here, as an employee and managing director of StoneX, Defendant had a fiduciary relationship to StoneX. *See Iacovacci v. Brevet Holdings, LLC*, 437 F. Supp. 3d 367, 381 (S.D.N.Y. 2020) (employer adequately alleged misappropriation of its trade secrets against the managing director with access to trade secrets).

Moreover, Defendant plainly engaged in misconduct that threatens to cause severe financial harm to StoneX. As discussed above, Defendant obtained StoneX's trade secrets through improper means, and is preventing StoneX from reclaiming those trade secrets, or even determining to full scope of trade secrets and other materials that Defendant stole. (CRA Decl. ¶¶ 18-20.) StoneX is damaged by this loss of its investment in developing and building Darwin and Pascal. Thus, StoneX is likely to succeed on the merits in proving Defendant owed and clearly breached his fiduciary duty to StoneX.

B. StoneX Will Suffer Irreparable Harm Without an Injunction

Should Defendant continue to possess and potentially disclose or destroy StoneX's trade secrets, StoneX will be irreparably harmed and unable to recuperate its losses through monetary damages. "Irreparable harm is defined as certain and imminent harm for which a monetary award does not adequately compensate." *Intertek Testing Servs., N.A. v. Pennisi*, 443 F. Supp. 3d 303, 328-29 (E.D.N.Y. 2020) (noting irreparable harm occurs "where the loss is difficult to replace or measure, or where plaintiffs should not be expected to suffer the loss."). StoneX will suffer irreparable harm absent an injunction because Defendant "does not merely seek to use its trade secrets or keep them to himself . . . [instead], he could disseminate the trade secrets he improperly acquired to a wider audience." *KCG Holdings, Inc. v. Khandekar*, No. 17-CV3533(AJN), 2020 WL 1189302, at *17 (S.D.N.Y. Mar. 12, 2020); *Syntel Sterling Best Shores Mauritius Ltd. v. TriZetto Grp., Inc.*, No. 15 Civ. 211(LGS), 2021 WL 1553926, at *13 (S.D.N.Y. Apr. 20, 2021) ("TriZetto has demonstrated irreparable harm . . . specifically the likelihood that, if not enjoined, Syntel will disseminate or impair the trade secrets by sharing them with unauthorized third parties."); *Chadha v. Chadha*, 2020 WL 1031385, at *15 (E.D.N.Y. Mar. 2, 2020) (finding irreparable harm where a plaintiff has no control over the use and dissemination of the stolen information). The loss of trade secrets is a recognized form of irreparable harm under New York law. *Intertek Testing Services, N.A.*, 443 F. Supp. 3d at 331; *FMC Corp. v. Taiwan Tainan Giant Indus. Co.*, 730 F.2d 61, 63 (2d Cir. 1984) ("[I]t is clear that the loss of trade secrets cannot be measured in money damages . . . A trade secret once lost is, of course, lost forever."

As long as Defendant possesses the 87MBs of information that he took from the Pascal Azure server and the two external hard drives with Stonex's information from his StoneX laptop, StoneX suffers irreparable harm with an increasing risk of future harm from disclosures. Further, StoneX has been unable to locate a copy of the Darwin source code as presented on December 9, 2022. (Pfeuffer Decl. ¶ 15.) StoneX similarly is unable to determine exactly what was included in the 87 MBs Defendant egressed and where it was sent. (Kolb Decl. ¶ 9.) The egress of StoneX's programs and data, plus Defendant deleting the bash history to prevent StoneX from determining where the data was sent, creates a very real risk that Defendant will be able to use "the knowledge he gleaned from his improper acquisition . . . to develop" systems and software at a competitor, or will use the information for some illegal purpose. *KCG Holdings, Inc.*, 2020 WL 1189302 at *17. Such information that is of great value to StoneX cannot be measured in money damages and thus causes irreparable injury. *FMC Corp.,* 730 F.2d at 63.

The highly technical manner that Defendant used to remove 87MBs from the Pascal Azure servers also creates a presumption of irreparable harm, which is "particularly appropriate when information of disclosure is highly technical or can be used only by a few specialized businesses." *KCG Holdings, Inc.*, 2020 WL 1189032, at *16; *Credit Suisse Sec. (USA) LLC v. Ebling*, No. 06 Civ. 11339(RCC), 2006 WL 3457693, at *1 (S.D.N.Y. Nov. 27, 2006) (TRO was granted compelling defendant and all those acting in concert with him to return immediately all confidential information and trade secrets that defendant unlawfully took from his employer); *Ayco Co. v. Feldman*, No. 1:10-CV-1213(GLS/DRH), 2010 WL 4286154, at *1 (N.D.N.Y. Oct. 22, 2010) (temporary restraining order "requiring the immediate return of any [confidential information and trade secrets] in Defendant's possession").

C. The Balance of Hardships Weighs Heavily in StoneX's Favor

Ordering Defendant to return StoneX's confidential and trade secret information will impose no hardship on Defendant but will mitigate substantial and irreparable injury to StoneX's business. *See Mission Cap. Advisors LLC v. Romaka*, No. 16 Civ. 5878(LLS), 2016 WL 11517104, at *2 (S.D.N.Y. July 29, 2016) ("Plaintiff avers that dissemination of the [trade secrets] would cause irreparable harm to Plaintiff, its business activities, and its market share, which could cause loss of revenue and competitive advantage. Defendant has no legitimate interest in Plaintiff's Contact Lists.").

Defendant has no *legitimate* interests that would be harmed by entry of the requested injunction, whereas StoneX continues to face significant irreparable harm if Defendant is not enjoined from using or disseminating StoneX's confidential and trade secret information, including Pascal and Darwin. Further, Defendant agreed to comply with StoneX's Exit Procedures, which include the obligation "not [to] delete any data which belongs to the Company" and to "transfer any data which may be needed by the Company to an appropriate server or colleague prior to departure." (Wareman Decl. ¶ 9.) *See Mickey's Linen v. Fischer*, No. 17 C 2154, 2017 WL 3970593, at *19 (N.D. Ill. Sept. 8, 2017) (holding that balance of harms weighed in favor of former employer and granting preliminary injunction to former employer in trade secrets case); *Mazak Optonics Corp. v. Marlette*, No. 17 C 1023, 2017 WL 3394727, at *3 (N.D. Ill. Aug. 8, 2017) (same).

This Court must require Defendant to return the confidential and trade secret information that he has no legitimate right to possess, to refrain from further disseminating the misappropriated information, and to not destroy evidence of his misconduct, which poses no burden to Defendant. *See Citizens Sec., Inc. v. Bender*, No. 1:19-cv-916(MAD/DJS), 2019 WL 3494397, at *5 (N.D.N.Y. Aug. 1, 2019) ("Plaintiff will continue to suffer substantial harm absent an injunction through Defendant's use of proprietary information to . . . Defendant, however, will only suffer minimal harm if an injunction is granted.").

D. Injunctive Relief Serves the Public Interest

Public interest would be served in granting the temporary restraining order against Defendant. "Injunctive relief would serve the public interest by . . . protecting plaintiff's legitimate interests in maintaining . . . the secrecy of its trade secrets and confidential information." *Intertek Testing Servs., N.A. v. Pennisi*, 443 F. Supp. 3d 303, 347 (E.D.N.Y. 2020); *see also Mazak Optonics Corp. v. Marlette*, No. 17 C 1023, 2017 WL 3394727, at *3 (N.D. Ill. Aug. 8, 2017) (The "public interest is supported by upholding the sanctity of confidential information such as trade secrets and preventing others from the unauthorized use of such confidential information for their own benefit.") Here, preventing Defendant's unauthorized possession, use or disclosure of StoneX's confidential business information and trade secrets serves the public interest.

CONCLUSION

StoneX therefore requests a temporary restraining order, consistent with the accompanying Proposed Order, enjoining Defendant from using, relying upon, or disseminating StoneX's confidential and trade secret information. Further, Defendant should be ordered to immediately return and not retain copies of StoneX's confidential information in his possession or under his control.

Dated: January 19, 2023

New York, New York

PROSKAUER ROSE LLP

/s/

Lloyd B. Chinn
Daryl Leon
Eleven Times Square
New York, New York 10036-8299
212.969.3000
lchinn@proskauer.com
dleon@proskauer.com

Nigel F. Telman (*pro hac vice* forthcoming)
Steven J. Pearlman (*pro hac vice* forthcoming)
Three First National Plaza
Chicago, Illinois 60602-4342
312.962.3548
ntelman@proskauer.com
spearlman@proskauer.com

Attorneys for Plaintiffs StoneX Group, Inc. and StoneX Financial, Inc.